The Honorable Richard A. Jones

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff<br><br>v.<br><br>ROMAN V. SELEZNEV,<br><br>Defendant. | NO. CR11-0070RAJ<br><br>**GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO SUPPRESS** |

## I. INTRODUCTION

Defendant moves the Court to suppress evidence obtained from the laptop computer that he was carrying at the time he was captured in the Maldives. The primary argument he raises in support of suppression is a claim of government misconduct in the handling of the computer prior to the forensic examination. Defendant's theory of suppression is a moving target. His request for leave to file a late motion indicated he was seeking to suppress the laptop based on alleged Fourth Amendment violations involving "unreasonable warrantless searches." Def. Motion for Leave, Dkt. 297 at 3, 5-6. He has now abandoned these allegations and argues that the government's alleged mishandling of the computer amounts to a due process violation that requires suppression. When a defendant seeks to suppress evidence based on claims of



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

government misconduct, the defendant must show the government acted in bad faith and demonstrate prejudice to his defense. *See Arizona v. Youngblood*, 488 U.S. 51 (1988); *United States v. Loud Hawk*, 628 F.2d 1139, 1152 (9th Cir. 1979). Defendant's proffered expert testimony is insufficient to establish any misconduct, let alone bad faith. The government's rebuttal expert testimony will fully explain and justify the government's conduct. Defendant's additional challenges based on staleness and delay in obtaining the warrant are equally without merit. Based on the totality of the circumstances, the government obtained a warrant within a reasonable amount of time. Furthermore, the affidavit in support of the warrant described overwhelming evidence that defendant's computer contained evidence of his crimes.

## II. FACTS

The government expects to establish the following facts at the evidentiary hearing scheduled for June 1-2, 2016. The government will present testimony from three witnesses: Special Agents Michael Fischlin and David Mills, and computer forensic expert Ovie Carroll, Director of the Department of Justice Cybercrime Laboratory.

### A. Seizure and Search Warrant Affidavit

On July 5, 2014, defendant was apprehended in the Maldives and transported to Guam for his initial appearance. At the time of his apprehension, defendant was carrying several electronic devices including a Sony Vaio laptop computer ("the computer"). Special Agent Daniel Schwandner inventoried the items and Special Agents Mark Smith and David Iacovetti confirmed the inventory while they were flying to Guam. Agent Iacovetti maintained custody of the items until he delivered them to the Seattle United States Secret Service (USSS) Field Office's evidence vault on July 8th. The following day, Agents Fischlin and Mills moved the computer to a separate USSS Electronic Crimes Task Force (ECTF) evidence vault in anticipation of a forensic examination. On the same day, while locating the computer's serial number, Agent Mills observed the computer's screen light up – which he reported in his examination notes. (*See* Def. Ex. 3 at 6). Although the screen lit up, the agents left the computer powered on because they



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

believed there was a high likelihood that defendant, a notorious and skilled cybercriminal, would have enabled encryption on his computer. In the agents' experience, powering down an encrypted computer would have left them with no means to break the encryption without the password. On the other hand, the agents were aware that there were possible methods to glean the encryption keys from a powered computer's random access memory (RAM). RAM, unlike a computer's hard drive, is volatile and cannot be recovered after the computer is powered down. (*See* Def.'s Exhibit 1 at ¶ 26). RAM can have significant forensic value because it may contain information (particularly very recent information not available elsewhere on the computer). *Id*. Forensic examiners, therefore, will occasionally attempt to conduct a "live image" of RAM in order to copy its data, including potential encryption keys.

As a result of the time between the defendant's 2011 indictment and his apprehension, neither the original case agent nor the original AUSA remained employed by the government. This meant that a new case agent and a new AUSA had to get up to speed on this complex case to prepare the search warrant. After the computer arrived in Seattle, Agent Fischlin immediately began working on a search warrant affidavit and submitted an initial draft to the U.S. Attorney's Office ("USAO") for review on July 10th. Between July 10th and July 22nd, Agent Fischlin consulted with the USAO and shared multiple drafts of his affidavit. Because he had only recently been assigned to the investigation, he needed time to familiarize himself with the case in order to respond to comments and edits from the USAO. On July 20th, however, Agent Fischlin traveled to Guam to testify at defendant's identity hearing scheduled for July 22nd. Over the next several days, the hearing was delayed repeatedly based on defense motions to continue and weather related closures of the court. As a result, Agent Fischlin stayed in Guam through July 30th, when the hearing went forward. Because Agent Fischlin was delayed in Guam and unavailable, USSS took the extraordinary step of arranging for another agent to travel from Washington D.C. exclusively for the purpose of swearing out the warrant. On Thursday July 24th, Special Agent Richard LaTulip from the Cyber



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Intelligence Section at USSS headquarters in Washington D.C., began revising the affidavit so that he could present the warrant application in place of Agent Fischlin. Agent LaTulip traveled to Seattle on July 28th, and presented the warrant to the Honorable James P. Donohue, who signed the warrant.

The search warrant affidavit details a multi-year, international investigation of a complex cybercrime scheme. The affidavit describes overwhelming evidence tying defendant to the infrastructure that supported his scheme between approximately 2007 and July 2014, including receipts with defendant's name, phone number and home address located in e-mail accounts used to manage defendant's criminal infrastructure. (*See* Def. Ex. 1 at ¶ 60, 82-83). The affidavit also described how defendant's internet travel reservations (including his date of birth and passport number) were located in the internet history of computer servers used to facilitate defendant's hacking scheme. (*See* Def. Ex. 1 at ¶'s 61-70). The affidavit also described evidence of recent credit card hacking and trafficking occurring up through the week before defendant's apprehension that was directly tied to defendant's past hacking and credit card trafficking through online currency accounts. (*See* Def. Ex. 1 at ¶ 57, 95-102, 105). In addition, the agent offered extensive background information related to how cybercriminals operate, including the fact that cybercriminals retain information related to their online user names/identities, otherwise known as "nics," over the course of several years. (*See* Def. Ex. 1 at ¶ 25). Indeed, the search of defendant's computer revealed he maintained lists documenting many of the usernames and passwords he had used continuously throughout his career, including key nics such as Bulba, 2pac, and smaus, and favorite passwords such as ochko123 and smaus123. (*See* Gov. Ex. 1 – User Credentials Files from Defendant's Computer).

**B. Storage and Forensic Examination of the Computer**

The computer remained in the ECTF evidence vault until July 30th, when Agent Mills removed the computer from the vault for the purpose of conducting a forensic examination. As of July 30th, Agent Mills anticipated conducting a live imaging of the



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

computer in an attempt to capture the RAM and any possible encryption keys it contained. (*See* Gov. Ex. 2 – Agent Mills Email, July 30, 2014). Upon retrieving the computer, however, Agent Mills noticed the computer appeared to be powered off. Therefore, he connected the computer to a power cable to recharge its battery in hopes that the RAM might be preserved. (*See* Def. Ex. at 6). That evening, Agent Mills sent an email to Agent Fischlin describing his efforts to research whether conducting a live image of the computer might be possible. (*See* Gov. Ex. 2). He explained that USSS had purchased a test machine similar to defendant's computer and that they had made several attempts to live image the test machine using different forensic products without success.

On August 1st, Agent Mills determined it would not be possible to conduct a live image and proceeded to dismantle the computer to remove the Solid State Drive (SSD) for forensic imaging. (*See* Def. Ex. at 7). While removing the back panel of the computer to access the SSD, Agent Mills noticed the screen of the computer light up and display the "splash screen" which he reported in his examination notes as occurring at approximately 2:45 PM PST (*See* Def. Ex. 3 at 4, 6). A forensic review of the computer revealed operating system activity consistent with this event at 2:48 PM PST. (*See* Def. Ex. 3 at 5). Agent Mills reported that this indicated "that the laptop, instead of being completely powered off, had been in a 'sleep' state." He then proceeded to power down the computer by pressing the power button and continued dismantling the computer. *Id.* After removing the SSD, Agent Mill's attached the SSD to an adapter and write blocker to begin the forensic imaging process at approximately 3:11 PM PST.

After making a forensic copy of the computer hard drive, Agent Mills found numerous files that had been automatically accessed by the computer's operating system after defendant's apprehension on July 5th, as well as numerous automatically generated files. Agent Mills reported this discovery in his report and summarized his research of the reasons why the computer showed activity following defendant's apprehension. (*See* Def. Ex. 5 at 6). Agent Mills explained that he learned that the operating system on the computer was Windows version 8.1 and this operating system may remain in a semi-



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

sleep mode as long as power is supplied. *Id.* When the device is in sleep mode, the operating system will continue to check or "write" files to the system. *Id.* Agent Mills opined that the only way to prevent this activity would be to physically remove the battery from the device which requires disassembly of the computer. *Id.*

**C. The Government's Independent Forensic Investigation**

In anticipation of defendant's allegations that the post-seizure file activity reported in Agent Mills examination affected the authenticity of the evidence on the computer, the government asked Mr. Carroll to independently review the forensic image of defendant's computer. Mr. Carroll examined every one of the files that were accessed or created on defendant's computer after his apprehension on July 5th, and determined that all of these files were accessed or created automatically by the operating system rather than any user input. (*See* Gov. Ex. 3 - Declaration of Ovie Carroll at ¶ 2, 4). Furthermore, he determined that none of the files accessed or created after defendant's apprehension had any impact on the authenticity of the exhibits the government intends to introduce. *Id*. at ¶ 7. Additionally, Mr. Carroll will testify that based on his examination of the computer system, event logs, registry and other forensic artifacts, he found the computer was last connected to a wireless network named "Kanifushi" (the name of the hotel at which defendant was staying immediately prior to his apprehension) on July 3rd, and that the evidence conclusively shows the computer did not connect to any other wired or wireless networks after July 3rd.

Mr. Carroll has also determined that the forensic evidence on the computer is entirely consistent with Agent Mill's examination reports, including the fact that the splash screen displayed on August 1st, as Agent Mills removed the back cover of the device. Mr. Carroll will testify that based on his training and experience, his knowledge of the Windows 8.1 Operating System, and his examination of the forensic evidence, he has determined that the computer was never fully powered down between July 5th and August 1st. He will explain how the system operated at low-battery levels, which caused the device to stop checking and/or writing files after July 14th. He will further explain



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

that contrary to defense expert Eric Blank's opinion that forensic evidence from the computer on August 1st demonstrated mishandling of the device during the imaging process, the forensic evidence, in fact, demonstrates Agent Mills imaging of the SSD was forensically sound. Finally, he will testify that Agent Mill's desire to conduct a live image of the device logically explains why it was maintained in a powered-on state between July 5th and August 1st, and why the agent plugged the device into power on July 30th, in anticipation of conducting a live image.

## III. ARGUMENT

### A. Defendant cannot meet his burden of showing government misconduct.

When seeking to suppress evidence based on allegations of government misconduct, defendant bears the burden of demonstrating bad faith and prejudice. *See United States v. Flyer*, 633 F.3d 911, 916 (9th Cir. 2011). Defendant's reliance on *United States v. Sivilla*, 714 F.3d 1168 (2013) to support a lower burden of proof is misplaced. In *Sivilla*, the defendant was charged with drug offenses after cocaine was found in the jeep he was driving. *See Sivilla*, 714 F.3d at 1170. Prior to trial, the district court ordered the government to preserve the vehicle as evidence. *See id.* Despite the order, the vehicle was auctioned and "stripped for parts." *Id*. at 1171. Defendant moved for dismissal of the indictment or, in the alternative, a remedial jury instruction based on the destruction of evidence. *Id*. The district court denied the motion to dismiss and refused the request for a remedial instruction based on the lack of bad faith. *Id*. The Ninth Circuit reversed regarding the jury instruction and found that "[b]ad faith [was] the wrong legal standard for a remedial jury instruction...." *Id*. at 1173. Instead, "[c]ourts must balance the quality of the Government's conduct against the degree of prejudice to the accused, where the government bears the burden of justifying its conduct and the accused of demonstrating prejudice." *Id*. (quoting *Loud Hawk*, 628 F.2d at 1152). Under that standard, the court held that a remedial jury instruction was warranted based on the government's destruction of evidence that may have been pivotal to the defense. *See id*. at 1173-74.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

The most obvious difference between this case and *Sivilla* is that in *Sivilla* evidence was destroyed in direct violation of a court order. *See id*. at 1170-71. In this case, defendant has not alleged nor shown any basis to believe evidence was destroyed – let alone in violation of a court order. Additionally, unlike in this case, *Sivilla* specified how the destroyed evidence would have been used by the defense – thereby demonstrating substantial prejudice to his defense. *See id*. at 1174. Here, defendant cannot show how any of the automatically updated files have any impact on his ability to present a defense. Finally, defendant is not simply seeking a remedial jury instruction – he is seeking the complete suppression of all evidence obtained from the computer. Because defendant cannot meet his burden of proving any misconduct, let alone bad faith, his motion must be denied.

The Ninth Circuit's decision in *Flyer* controls here. *Flyer*, 633 F.3d at 916. In *Flyer* the Ninth Circuit affirmed a district court's denial of a motion to suppress in which defendant argued that the forensic examiner's corruption of files on defendant's computer as a result of mistakenly allowing the examiner's computer to connect to the defendant's computer and change last accessed dates on relevant files, showed bad faith. *Id*. at 915-916. In that case, the forensic examiner belatedly admitted that he had mistakenly connected his computer to the defendant's laptop without proper write blocking during the forensic imaging process and changed the last access dates on over 69,000 files, including two that formed the basis of specific counts in the indictment. *Id*. The examiner did not mention the mistake at all in his report. Instead the examiner reported that "approved procedures and protocols were used," which he "later admitted to be false." *Id*. at 915. Because this resulted in the metadata for the two relevant files being overwritten, the government dismissed the counts in the indictment based on those files.[1]

---

[1] As a result of the change in the last accessed dates for the two child pornography files that the government alleged defendant had downloaded, they could no longer determine the correct last accessed dates for those files.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

*Id*. Nonetheless, the court found the government presented evidence that the agent did not intentionally corrupt the data, "but rather mishandled it" and that Flyer did not "show that mishandling of the evidence prejudiced his defense." *Id*. at 916. Therefore, the court affirmed the district court's denial of defendant's motion to suppress evidence.

Unlike the agent in *Flyer*, Agent Mills did not mishandle defendant's computer. The forensic evidence, contrary to defense expert's claims, shows no user interaction with defendant's computer or any errors in the imaging process such as those that occurred in *Flyer*. Additionally, Agent Mills specifically reported the file changes caused by the system in his initial report and a supplemental report providing additional details. (*See* Def. Ex. 3 at 5; Def. Ex. 2). Moreover, the agent's decision to keep the computer powered on between July 5, 2014, and the time of his examination was based on legitimate forensic goals – the goal of conducting a live image to preserve defendant's encryption keys. (*See* Gov. Ex. 2). Most importantly, unlike the changes to the metadata for the two files in *Flyer* that formed the sole basis of two counts in the indictment, none of the metadata changes in this case have any impact on the authenticity of the exhibits the government intends to introduce at trial, or on defendant's ability to present a defense. The only exhibits from the computer that the government intends to introduce as exhibits at trial consist of files and forensic artifacts that were created on the device prior to defendant's apprehension and were neither modified nor altered after defendant's apprehension.[2]

The forensic evidence from the computer establishes beyond any reasonable doubt that all of the exhibits from defendant's laptop computer are in the exact same condition

---

[2] One exhibit - a banner advertisement for defendant's carding website 2pac.cc, that was located on the desktop of defendant's operating system - shows a last accessed date of July 13, 2014. Mr. Carroll will explain that this was the result of routine system generated activity and resulted in no changes to the content of the file. None of the other exhibits from defendant's computer that the government has selected for trial were accessed by the operating system or any human user following defendant's apprehension.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

as they were at the time the computer was seized from defendant on July 5, 2014. Defendant's claim that the government mishandled, tampered with, or planted evidence on the computer is without any merit and fails to establish even simple negligence, let alone government misconduct amounting to bad faith that would be necessary to support the extraordinary remedy of suppression. Because the forensic examination of defendant's laptop computer confirms the integrity of the evidence located on the computer and proves no misconduct occurred, defendant's motion should be denied.

**B. Defendant's criticism of the forensic examination goes to the weight rather than the admissibility of the evidence found on the computer.**

The reliability and authenticity of the evidence discovered on defendant's computer is a disputed issue of fact that does not support exclusion of the evidence. At most, defendant's claims challenge the credibility of the witnesses and the reliability of the evidence. Any evidence or argument in support of these claims goes to the weight of the evidence rather than its admissibility. Such challenges to the government's evidence are properly reserved for presentation to the ultimate finder of fact – the jury.

Mr. Blank's claim that the file date changes suggest the possibility of evidence tampering or mishandling is insufficient as a matter of law to support exclusion of the evidence. Mr. Blank's opinion is based on the premise that the file date changes on the computer were the result of user interaction. Because the forensic evidence establishes that his premise is false, his entire opinion is without merit – and should be excluded at trial. Nonetheless, he argues that because computer data can be changed or deleted and that an experienced user can cover up such activity, it would be unreasonable to rely on any files on the computer despite the absence of any evidence demonstrating changes to the relevant files. This argument is directly contrary to established Ninth Circuit precedent. As that court has held "[t]he fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility that the logs may have been altered goes only to the weight of the evidence not its admissibility." *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir.1988); *see also*,



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

*United States v. Glasser*, 773 F.2d 1553 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records."); *United States v. Safavian*, 435 F.Supp.2d 36, 39–40 (D.D.C.2006) ("The possibility of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents).")

**C. The affidavit established a direct tie between defendant's past computer hacking activity and credit card trafficking and recent criminal behavior the week before his 2014 apprehension and, therefore, was not stale.**

Before a warrant is issued, the Fourth Amendment requires a neutral and detached judge to find the facts and circumstances presented in an affidavit are "'sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed,' and that evidence bearing on that offense will be found in the place to be searched." *Safford Unified School Dist. No. 1 v. Redding*, 129 S.Ct. 2633, 2639 (2009) (citations omitted). This requirement is a "'practical, nontechnical conception' that deals with 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.'" *Maryland v. Pringle*, 540 U.S. 366, 370 (2003) (quoting *Illinois v. Gates*, 462 U.S. 213, 231 (1983)). Probable cause does not require a showing of "certainty or even a preponderance of the evidence." *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006) (en banc). It requires only a "'fair probability' that contraband or evidence is located in a particular place," a finding that, in turn, depends on "the totality of the circumstances, including reasonable inferences and is a 'common sense, practical question.'" *United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2003) (quoting *Gourde*, 440 F.3d at 1069).

An affidavit in support of a search warrant must also be based on facts "'so closely related to the time of the issue of the warrant as to justify a finding of probable cause at



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

that time.'" *United States v. Lacy*, 119 F.3d 742, 745-46 (9th Cir. 1997) (quoting *Durham v. United States*, 403 F.2d 190, 193 (9th Cir. 1968)). The court must evaluate claims of staleness, however, "in light of the particular facts of the case and the nature of the criminal activity and property sought." *Id*. (quoting *United States v. Pitts*, 6 F.3d 1366, 1369 (9th Cir. 1993). The mere passage of time is not controlling and a search warrant is "not stale if 'there is sufficient basis to believe, based on a continuing pattern or other good reasons, that the items to be seized are still on the premises." *Id*. (quoting *United States v. Gann*, 732 F.2d 714, 722 (9th Cir. 1984). While staleness "is highly relevant to the legality of a search for a perishable or consumable object, like cocaine," it is "rarely relevant when it is a computer file" because computers and computer equipment are "not the type of evidence that rapidly dissipates or degrades." *United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012) (quoting *United States v. Vosburgh*, 602 F.3d 512, 529 (3rd Cir. 2010). As the Ninth Circuit has observed, computers have "long memor[ies]." *Gourde*, 440 F.3d at 1071.

Here, the information set forth in the affidavit provided more than sufficient probable cause to believe the evidence sought would be located on defendant's computer and other electronic devices. Much like the agent in *Lacy*, Agent LaTulip provided information based on his training and experience that cybercriminals maintain their online identities and information related to the criminal behavior for long periods of time. *Lacy*, 119 F.3d at 746 (noting agent's statement that collectors of child pornography value their materials and store them for long periods of time); (*see* Def. Ex. 1 at ¶ 25) (noting that cybercriminals jealously guard and protect their online identities and, as a result, evidence of a particular cybercriminal's identity may be found on digital devices and electronic storage media used over many years). Agent LaTulip also provided extensive details related to defendant's e-currency accounts used to facilitate his cybercrime scheme over several years and carefully explained tracing the use of those accounts to a new credit card vending site that was operating up through the week prior to defendant's apprehension. (*See* Def. Ex. 1 at ¶ 57, 95-102, 105). This evidence provided



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

direct evidentiary connections between defendant's earlier hacking and credit card trafficking and ongoing hacking and credit card trafficking in the weeks leading up to defendant's apprehension, and required no evidentiary inferences to find probable case. Agent LaTulip also explained that undercover purchases through July 2014, confirmed defendant was trafficking in stolen credit cards on his new vending site 2pac.cc, providing further direct evidence in support of probable cause. (*See* Def. Ex. 1 at ¶ 97). Finally, Agent LaTulip also noted that upon defendant's apprehension, the administrator of the 2pac site, who had previously been active in posting updates to the site, mysteriously stopped posting between July 5 and July 21, 2014. (*See* Def. Ex. 1 at ¶ 105). This powerful circumstantial evidence supported a strong inference that defendant was responsible for maintaining the 2pac.cc vending site as some observers in the media also noticed at the time. (*See* Gov. Ex. 4 – Seleznev Arrest Explains '2pac' Downtime, KrebsonSecurity, October 15, 2014, available at http://krebsonsecurity.com/2014/10/seleznev-arrest-explains-2pac-downtime/). Therefore, the totality of the circumstances, including the reasonable inferences that may be drawn from the affidavit, establish probable cause closely related to the time of the issue of the warrant requiring the Court to reject defendant's claims of staleness.

**D. The 23-day period in obtaining the warrant was reasonable.**

When determining whether the "delay between seizure of a package and obtaining a search warrant may violate the defendant's Fourth Amendment rights…the touchstone is reasonableness." *United States v. Sullivan*, 797 F.3d 623, 633 (9th Cir. 2015) (citing *United States v. Van Leeuwen*, 397 U.S. 249, 252-53 (1970)). Reasonableness is determined under the "totality of the circumstances, [and] not whether the Government pursued the least intrusive course of action." *United States v. Hernandez*, 313 F.3d 1206, 1213 (9th Cir. 2002). Moreover, the Court must balance "the nature and quality of the intrusion of the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." *Sullivan*, 797 F.3d at 633 (quoting *United States v. Place*, 462 U.S. 696 (1983)). In assessing case specific facts,



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

courts have examined factors such as defendant's failure to seek a return of his property, custodial status, parole, consent, weekends and holidays, higher priority cases and the diligence of the investigating agents in seeking a warrant. *See Sullivan*, 797 F.3d at 633 (21-day delay was reasonable, in part because defendant was in custody on a parole violation, defendant gave consent to search, and defendant never sought the return of his laptop); *United States v. Martin*, 157 F.3d 46, 54 (2nd Cir. 1998) (11-day delay was reasonable, in part, because the delay included two weekends and the Christmas holiday. The court also considered that the item had been sent to a co-conspirator via UPS); *United States v. Stabile*, 633 F.3d 219, 235-236 (3rd Cir. 2011) (3-month delay was reasonable where defendant had consented to the search and investigating Secret Service agent was assigned to protect the President and other high-ranking officials); *United States v. Howe*, 545 Fed.Appx. 64, 66 (2nd Cir. 2013) (13-month delay was reasonable, in part because of the government's strong interest in keeping a computer on which law enforcement had observed child pornography, and because delay was based on a mistake by the case agent that a state warrant had been obtained to search the computer); *United States v. Christie*, 717 F.3d 1156, 1164 (10th Cir. 2013) (5-month delay was reasonable after defendant consented and never sought return, and investigating agent was delayed due to other law enforcement priorities). As the case law suggests, no single fact is dispositive, and this Court should assess the specific facts of this case in determining whether the 23-day period of time was reasonable.

Here, the government confronted unusual obstacles in preparing the warrant. Neither the original case agent nor the original AUSA could perform these tasks. Further, the new case agent was required to spend approximately two weeks in Guam addressing defendant's custodial status. In light of this background, the government's efforts were diligent. The computer was seized from the defendant on July 5, 2014, while defendant was in the Republic of the Maldives. The defendant and the computer were flown to Guam that same day. Defendant has been in custody continuously since July 5, 2014, and never sought the return of his computer. The computer was delivered to



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Seattle on July 8th, and Agent Fischlin immediately began preparing a search warrant – sending a first draft to the USAO on July 10th. Between then and July 20th (which included two weekends), Agent Fischlin and the USAO consulted on multiple drafts. During that time, Agent Fischlin had to learn the facts of this complex case, as the agent who originally investigated the case had left government employment. Then, on July 20th, Agent Fischlin had to stop his efforts to travel to Guam where defendant was scheduled for an identity hearing on July 22nd. Because he was delayed in Guam as a result of defense motions and weather-related closures of the courthouse, Agent Fischlin sought the assistance of Agent LaTulip in Washington D.C., who had some familiarity with the case. Agent LaTulip traveled from Washington D.C. to Seattle and swore out the warrant on July 28th. In short, within 23 days, defendant's computer traveled from the Republic of Maldives, to Guam, to Seattle, the case agent traveled from Seattle to Guam, and in an effort to expedite the warrant, the case agent took the extraordinary step of asking an agent to travel from Washington D.C. to Seattle to swear out the affidavit.[3]

In light of the totality of the circumstances, the fact that it only took 23 days to obtain a warrant is entirely reasonable. First, defendant's possessory interest in the computer was minimal because defendant was in custody and made no request for the return of his computer. Moreover, as this Court already found, it had already been lawfully seized. Second, the government had a substantial and legitimate interest in the contents of the computer as evidence as it was extremely likely to contain significant evidence of the crimes under investigation. Third, the agents acted diligently in pursuing a warrant and the totality of the circumstances - including the agent's lack of familiarity with the investigation, his need to review a complex multi-year investigation, his other duties including preparing for and appearing at defendant's identity hearing several thousand miles away, the complexity of the warrant affidavit, and the fact that the agent

[3] No other agents in Seattle had sufficient familiarity with the case to make them available to stand-in for Agent Fischlin.



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

requested outside assistance when he was delayed in Guam – all show that the 23 day delay to obtain a warrant in this case was reasonable.

Defendant unpersuasively relies on *United States v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009) and *United States v. Dass*, 849 F.2d 414 (9th Cir 1988) – two cases with vastly different facts from those found here. In *Mitchell*, the Eleventh Circuit found a 21 day delay to obtain a warrant unreasonable in light of the simple nature of the investigation, the fact that the affidavit consisted largely of boilerplate language, and the fact that another agent familiar with the facts was available to draft the warrant earlier. *Mitchell*, 565 F.3d at 1351. In *Dass*, the Ninth Circuit addressed whether it was reasonable for the government to hold items seized from the mail for up to 23 days in order to seek warrants based on the fact that a dog's sniff had indicated the presence of marijuana. *Dass*, 849 F.2d at 414-415. Neither of these cases resembles the facts that are at issue in this case.

*Mitchell* involved a much less complicated investigation and a lack of diligence on the part of law enforcement – including a failure to seek assistance from other agents. *Mitchell*, 565 F.3d at 1351-1353. The Eleventh Circuit has since found a more substantial delay was reasonable in light of facts more similar to those in this case. In *United States v. Laist*, 702 F.3d 608, 613-616 (11th Cir. 2012) the court distinguished *Mitchell* and found a 25-day delay in obtaining a warrant was reasonable, in part, because defendant initially consented to a search, defendant had the opportunity to copy items from his computer, law enforcement observed contraband on the computer, the case was complex and the agent worked diligently in obtaining the warrant. The court commended the agent's efforts to "put the ball in motion the very first day that he received the notice" that the defendant had revoked consent, and submitted a first draft of his affidavit to the U.S. Attorney's Office 10 days later – with the record demonstrating the agent and prosecutor exchanged edits in the weeks leading up to the warrant's presentation to the Magistrate Judge. *Id*. at 617. Here, Agent Mills submitted an initial draft to the U.S. Attorney's Office within two days of the computer's arrival in Seattle. The *Laist* court also noted that "an investigation of this scope and complexity requires more time to



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

prepare a warrant" and cited the fact that the investigation had taken "roughly a year and involved the efforts of numerous FBI agents besides [the case agent], rendering it unlike a simpler case such as some narcotics possession cases." *Id.* While the *Laist* investigation involved a relatively complex child pornography case, the investigation here was even more complex – involving a multi-year, international investigation with multiple search warrants and extensive forensic evidence. Finally, the *Laist* court also noted the fact that the agents were extremely busy with other matters. *Id.* Agent Fischlin was similarly busy as a result of other duties related to this very investigation including the need to travel several thousand miles to testify at defendant's identity hearing.

*Dass* is similarly unhelpful to the analysis in this case. The detention of a mailed package for up to 23 days to obtain a warrant that need only describe a dog sniff is nothing like the detention of a lawfully seized computer for 23 days in which the agent must describe a complex international cybercrime investigation. As an initial matter, the detention of mail that a recipient expects to receive in a relatively short time period amounts to a substantial intrusion on the individual's Fourth Amendment interests that is not present in this case. *See Sullivan*, 797 F.3d 623, 633. In *Sullivan*, the Ninth Circuit distinguished *Dass* and *Mitchell* in a case involving the seizure of a computer from a defendant who remained in custody throughout the time the government pursued a warrant. *Id.* Distinguishing *Dass*, the court found a 21-day delay in obtaining a warrant was reasonable and that defendant's possessory interest, given the totality of the circumstances, was minimal noting "where individuals are incarcerated and cannot make use of seized property, their possessory interest in that property is reduced. *Id.* (citing *Segura v. United States*, 468 U.S. 796, 813 (1984). The court went on to distinguish *Mitchell*, noting that *Sullivan* made no argument that he had "made any request for the laptop's return, and had a reduced possessory interest due to his status as a parolee." *Id.* at 635. On the other side of the balance, the court found the government had a "reasonable basis for its delay, including the need to transfer the laptop between agencies" to execute the search. The court also noted *Mitchell's* suggestion that asking



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

for the assistance of another law enforcement officer, as Agent Fischlin did here, strengthens the reasonableness of the government's delay. *Id*. (citing *Mitchell*, 702 F.3d at 1352-53). Therefore, the totality of the circumstances in this case shows that the delay in obtaining the warrant was reasonable and defendant's argument should be rejected.

**E. The agents acted in good faith reliance on a facially valid warrant.**

*United States v. Leon*, 468 U.S. 897, 922 25 (1984), holds that if the police conduct a search relying, in good faith, upon a judge's issuance of a warrant, evidence obtained during that search will not be subject to suppression even if it is later determined the judge erred in issuing the warrant. This "good faith exception will save a search based on a defective warrant *unless no reasonable police officer could have believed there was probable cause* to search the location identified in the search warrant." *United States v. Chavez Miranda*, 306 F.3d 973, 980 n.3 (9th Cir. 2002) (emphasis added). In *Leon*, the Supreme Court listed four circumstances in which the good faith exception will not apply: 1) when the magistrate was misled by information in the affidavit the affiant knew or should have known was false, 2) when the magistrate has wholly abandoned her judicial role, 3) when the affidavit is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable, and 4) when the warrant is so facially deficient —i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid. *Id*. at 923, 104 S.Ct. at 3421. None of the *Leon* exceptions applies to this case. There was no use of materially misleading information in the affidavit. There is no evidence that the magistrate wholly abandoned his judicial role, and, as discussed above, there was ample probable cause to search. Additionally, defendant makes no colorable claim that the warrant was so sweeping as to be facially invalid.

## IV. CONCLUSION

Defendant cannot meet his burden of proving any government misconduct in the handling of the computer. The warrant was based on ample probable cause demonstrating ongoing criminal activity and a basis to believe evidence would be located



UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

on the computer. The delay in obtaining the warrant is reasonable in light of the totality of the circumstances. Accordingly, defendant's motion to suppress should be denied.

DATED this 17th day of May, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

*s/ Norman M. Barbosa*
NORMAN M. BARBOSA

*s/ Seth Wilkinson*
SETH WILKINSON

Assistant United States Attorneys
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Email: Norman.Barbosa@usdoj.gov
Email: Seth.Wilkinson@usdoj.gov

LESLIE R. CALDWELL
Assistant Attorney General

*s/ Harold Chun*
HAROLD CHUN
Trial Attorney
Computer Crime and Intellectual Property Section
1301 New York Avenue, NW
Washington, D.C. 20530
Email: Harold.Chun@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on May 17, 2016, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the attorney of record for the defendant.

*s/Janet K. Vos*
JANET K. VOS
Paralegal Specialist
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-7970
Fax: (206) 553-0755
E-mail: Janet.Vos@usdoj.gov